

SECURELY PROTECT YOURSELF AGAINST CYBER  
TRESPASS ACT (SPY ACT)

MAY 24, 2007.—Committed to the Committee of the Whole House on the State of  
the Union and ordered to be printed

Mr. DINGELL, from the Committee on Energy and Commerce,  
submitted the following

R E P O R T

[To accompany H.R. 964]

[Including cost estimate of the Congressional Budget Office]

The Committee on Energy and Commerce, to whom was referred  
the bill (H.R. 964) to protect users of the Internet from unknowing  
transmission of their personally identifiable information through  
spyware programs, and for other purposes, having considered the  
same, report favorably thereon with an amendment and rec-  
ommend that the bill as amended do pass.

CONTENTS

	Page
Purpose and Summary .....	10
Background and Need for Legislation .....	10
Hearings .....	12
Committee Consideration .....	12
Committee Votes .....	13
Committee Oversight Findings .....	13
Statement of General Performance Goals and Objectives .....	13
New Budget Authority, Entitlement Authority, and Tax Expenditures .....	13
Earmarks and Tax and Tariff Benefits .....	13
Committee Cost Estimate .....	13
Congressional Budget Office Estimate .....	13
Federal Mandates Statement .....	16
Advisory Committee Statement .....	16
Constitutional Authority Statement .....	16
Applicability to Legislative Branch .....	16
Section-by-Section Analysis of the Legislation .....	16
Changes in Existing Law Made by the Bill, as Reported .....	26

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the “Securely Protect Yourself Against Cyber Trespass  
Act” or the “Spy Act”.

**SEC. 2. PROHIBITION OF UNFAIR OR DECEPTIVE ACTS OR PRACTICES RELATING TO SPYWARE.**

(a) **PROHIBITION.**—It is unlawful for any person, who is not the owner or authorized user of a protected computer, to engage in unfair or deceptive acts or practices that involve any of the following conduct with respect to the protected computer:

- (1) Taking control of the computer by—
  - (A) utilizing such computer to send unsolicited information or material from the computer to others;
  - (B) diverting the Internet browser of the computer, or similar program of the computer used to access and navigate the Internet—
    - (i) without authorization of the owner or authorized user of the computer; and
    - (ii) away from the site the user intended to view, to one or more other Web pages, such that the user is prevented from viewing the content at the intended Web page, unless such diverting is otherwise authorized;
  - (C) accessing, hijacking, or otherwise using the modem, or Internet connection or service, for the computer and thereby causing damage to the computer or causing the owner or authorized user or a third party defrauded by such conduct to incur charges or other costs for a service that is not authorized by such owner or authorized user;
  - (D) using the computer as part of an activity performed by a group of computers that causes damage to another computer; or
  - (E) delivering advertisements or a series of advertisements that a user of the computer cannot close or terminate without undue effort or knowledge by the user or without turning off the computer or closing all sessions of the Internet browser for the computer.
- (2) Modifying settings related to use of the computer or to the computer's access to or use of the Internet by altering—
  - (A) the Web page that appears when the owner or authorized user launches an Internet browser or similar program used to access and navigate the Internet;
  - (B) the default provider used to access or search the Internet, or other existing Internet connections settings;
  - (C) a list of bookmarks used by the computer to access Web pages; or
  - (D) security or other settings of the computer that protect information about the owner or authorized user for the purposes of causing damage or harm to the computer or owner or user.
- (3) Collecting personally identifiable information through the use of a keystroke logging function.
- (4) Inducing the owner or authorized user of the computer to disclose personally identifiable information by means of a Web page that—
  - (A) is substantially similar to a Web page established or provided by another person; and
  - (B) misleads the owner or authorized user that such Web page is provided by such other person.
- (5) Inducing the owner or authorized user to install a component of computer software onto the computer, or preventing reasonable efforts to block the installation or execution of, or to disable, a component of computer software by—
  - (A) presenting the owner or authorized user with an option to decline installation of such a component such that, when the option is selected by the owner or authorized user or when the owner or authorized user reasonably attempts to decline the installation, the installation nevertheless proceeds; or
  - (B) causing such a component that the owner or authorized user has properly removed or disabled to automatically reinstall or reactivate on the computer.
- (6) Misrepresenting that installing a separate component of computer software or providing log-in and password information is necessary for security or privacy reasons, or that installing a separate component of computer software is necessary to open, view, or play a particular type of content.
- (7) Inducing the owner or authorized user to install or execute computer software by misrepresenting the identity or authority of the person or entity providing the computer software to the owner or user.
- (8) Inducing the owner or authorized user to provide personally identifiable, password, or account information to another person—
  - (A) by misrepresenting the identity of the person seeking the information; or
  - (B) without the authority of the intended recipient of the information.

(9) Removing, disabling, or rendering inoperative a security, anti-spyware, or anti-virus technology installed on the computer.

(10) Installing or executing on the computer one or more additional components of computer software with the intent of causing a person to use such components in a way that violates any other provision of this section.

(b) GUIDANCE.—The Commission shall issue guidance regarding compliance with and violations of this section. This subsection shall take effect upon the date of the enactment of this Act.

(c) EFFECTIVE DATE.—Except as provided in subsection (b), this section shall take effect upon the expiration of the 6-month period that begins on the date of the enactment of this Act.

**SEC. 3. PROHIBITION OF COLLECTION OF CERTAIN INFORMATION WITHOUT NOTICE AND CONSENT.**

(a) OPT-IN REQUIREMENT.—Except as provided in subsection (e), it is unlawful for any person—

(1) to transmit to a protected computer, which is not owned by such person and for which such person is not an authorized user, any information collection program, unless—

(A) such information collection program provides notice in accordance with subsection (c) before downloading or installing any of the information collection program; and

(B) such information collection program includes the functions required under subsection (d); or

(2) to execute any information collection program installed on such a protected computer unless—

(A) before execution of any of the information collection functions of the program, the owner or an authorized user of the protected computer has consented to such execution pursuant to notice in accordance with subsection (c); and

(B) such information collection program includes the functions required under subsection (d).

(b) INFORMATION COLLECTION PROGRAM.—

(1) IN GENERAL.—For purposes of this section, the term “information collection program” means computer software that performs either of the following functions:

(A) COLLECTION OF PERSONALLY IDENTIFIABLE INFORMATION.—The computer software—

(i) collects personally identifiable information; and

(ii)(I) sends such information to a person other than the owner or authorized user of the computer, or

(II) uses such information to deliver advertising to, or display advertising on, the computer.

(B) COLLECTION OF INFORMATION REGARDING INTERNET ACTIVITY TO DELIVER ADVERTISING.—The computer software—

(i) collects information regarding the user’s Internet activity using the computer; and

(ii) uses such information to deliver advertising to, or display advertising on, the computer.

(2) EXCEPTION FOR SOFTWARE COLLECTING INFORMATION REGARDING INTERNET ACTIVITY WITHIN A PARTICULAR WEB SITE.—Computer software that otherwise would be considered an information collection program by reason of paragraph (1)(B) shall not be considered such a program if—

(A) the only information collected by the software regarding the user’s internet activity, and used to deliver advertising to, or display advertising on, the protected computer, is—

(i) information regarding Web pages within a particular Web site; or

(ii) in the case of any Internet-based search function, user-supplied search terms necessary to complete the search and return results to the user;

(B) such information collected is not sent to a person other than—

(i) the provider of the Web site accessed or Internet-based search function; or

(ii) a party authorized to facilitate the display or functionality of Web pages within the Web site accessed; and

(C) the only advertising delivered to or displayed on the computer using such information is advertising on Web pages within that particular Web site.

(c) NOTICE AND CONSENT.—

(1) IN GENERAL.—Notice in accordance with this subsection with respect to an information collection program is clear and conspicuous notice in plain language, set forth as the Commission shall provide, that meets all of the following requirements:

(A) The notice clearly distinguishes a statement required under subparagraph (B) from any other information visually presented contemporaneously on the computer.

(B) The notice contains one of the following statements, as applicable, or a substantially similar statement:

(i) With respect to an information collection program described in subsection (b)(1)(A): “This program will collect and transmit information about you. Do you accept?”.

(ii) With respect to an information collection program described in subsection (b)(1)(B): “This program will collect information about Web pages you access and will use that information to display advertising on your computer. Do you accept?”.

(iii) With respect to an information collection program that performs the actions described in both subparagraphs (A) and (B) of subsection (b)(1): “This program will collect and transmit information about you and will collect information about Web pages you access and use that information to display advertising on your computer. Do you accept?”.

(C) The notice provides for the user—

(i) to grant or deny consent referred to in subsection (a) by selecting an option to grant or deny such consent; and

(ii) to abandon or cancel the transmission or execution referred to in subsection (a) without granting or denying such consent.

(D) The notice provides an option for the user to select to display on the computer, before granting or denying consent using the option required under subparagraph (C), a clear description of—

(i) the types of information to be collected and sent (if any) by the information collection program;

(ii) the purpose for which such information is to be collected and sent; and

(iii) in the case of an information collection program that first executes any of the information collection functions of the program together with the first execution of other computer software, the identity of any such software that is an information collection program.

(E) The notice provides for concurrent display of the information required under subparagraphs (B) and (C) and the option required under subparagraph (D) until the user—

(i) grants or denies consent using the option required under subparagraph (C)(i);

(ii) abandons or cancels the transmission or execution pursuant to subparagraph (C)(ii); or

(iii) selects the option required under subparagraph (D).

(2) SINGLE NOTICE.—The Commission shall provide that, in the case in which multiple information collection programs are provided to the protected computer together, or as part of a suite of functionally related software, the notice requirements of paragraphs (1)(A) and (2)(A) of subsection (a) may be met by providing, before execution of any of the information collection functions of the programs, clear and conspicuous notice in plain language in accordance with paragraph (1) of this subsection by means of a single notice that applies to all such information collection programs, except that such notice shall provide the option under subparagraph (D) of paragraph (1) of this subsection with respect to each such information collection program.

(3) CHANGE IN INFORMATION COLLECTION.—If an owner or authorized user has granted consent to execution of an information collection program pursuant to a notice in accordance with this subsection:

(A) IN GENERAL.—No subsequent such notice is required, except as provided in subparagraph (B).

(B) SUBSEQUENT NOTICE.—The person who transmitted the program shall provide another notice in accordance with this subsection and obtain consent before such program may be used to collect or send information of a type or for a purpose that is materially different from, and outside the scope of, the type or purpose set forth in the initial or any previous notice.

(4) REGULATIONS.—The Commission shall issue regulations to carry out this subsection.

(d) **REQUIRED FUNCTIONS.**—The functions required under this subsection to be included in an information collection program that executes any information collection functions with respect to a protected computer are as follows:

(1) **DISABLING FUNCTION.**—With respect to any information collection program, a function of the program that allows a user of the program to remove the program or disable operation of the program with respect to such protected computer by a function that—

(A) is easily identifiable to a user of the computer; and

(B) can be performed without undue effort or knowledge by the user of the protected computer.

(2) **IDENTITY FUNCTION.**—

(A) **IN GENERAL.**—With respect only to an information collection program that uses information collected in the manner described in subparagraph (A)(ii)(II) or (B)(ii) of subsection (b)(1) and subject to subparagraph (B) of this paragraph, a function of the program that provides that each display of an advertisement directed or displayed using such information, when the owner or authorized user is accessing a Web page or online location other than of the provider of the computer software, is accompanied by the name of the information collection program, a logogram or trademark used for the exclusive purpose of identifying the program, or a statement or other information sufficient to clearly identify the program.

(B) **EXEMPTION FOR EMBEDDED ADVERTISEMENTS.**—The Commission shall, by regulation, exempt from the applicability of subparagraph (A) the embedded display of any advertisement on a Web page that contemporaneously displays other information.

(3) **RULEMAKING.**—The Commission may issue regulations to carry out this subsection.

(e) **LIMITATION ON LIABILITY.**—A telecommunications carrier, a provider of information service or interactive computer service, a cable operator, or a provider of transmission capability shall not be liable under this section to the extent that the carrier, operator, or provider—

(1) transmits, routes, hosts, stores, or provides connections for an information collection program through a system or network controlled or operated by or for the carrier, operator, or provider; or

(2) provides an information location tool, such as a directory, index, reference, pointer, or hypertext link, through which the owner or user of a protected computer locates an information collection program.

(f) **STUDY AND ADDITIONAL EXEMPTION.**—

(1) **STUDY AND REPORT.**—The Commission shall conduct a study to determine the applicability of the information collection prohibitions of this section to information that is input directly by users in a field provided on a website. The study shall examine—

(A) the nature of such fields for user input;

(B) the use of a user's information once input and whether such information is sent to a person other than the provider of the Web site;

(C) whether such information is used to deliver advertisements to the user's computer; and

(D) the extent of any notice provided to the user prior to such input.

(2) **REPORT.**—The Commission shall transmit a report on such study to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate not later than the expiration of the 6-month period that begins on the date on which final regulations are issued under section 9. The requirements of subchapter I of chapter 35 of title 44, United States Code, shall not apply to the report required under this subsection.

(3) **REGULATION.**—If the Commission finds that users have adequate notice regarding the uses of any information input directly by the user in a field provided on a website, such that an exemption from the requirements of this section, or a modification of the notice required by this section is appropriate for such information, and that such an exemption or modification is consistent with the public interest, the protection of consumers, and the purposes of this Act, the Commission may prescribe such an exemption or modification by regulation.

#### **SEC. 4. ENFORCEMENT.**

(a) **UNFAIR OR DECEPTIVE ACT OR PRACTICE.**—This Act shall be enforced by the Commission under the Federal Trade Commission Act (15 U.S.C. 41 et seq.). A violation of any provision of this Act or of a regulation issued under this Act shall be treated as an unfair or deceptive act or practice violating a rule promulgated under section 18 of the Federal Trade Commission Act (15 U.S.C. 57a).

## (b) PENALTY FOR PATTERN OR PRACTICE VIOLATIONS.—

(1) IN GENERAL.—Notwithstanding subsection (a) and the Federal Trade Commission Act, in the case of a person who engages in a pattern or practice that violates section 2 or 3, the Commission may, in its discretion, seek a civil penalty for such pattern or practice of violations in an amount, as determined by the Commission, of not more than—

- (A) \$3,000,000 for each violation of section 2; and
- (B) \$1,000,000 for each violation of section 3.

## (2) TREATMENT OF SINGLE ACTION OR CONDUCT.—In applying paragraph (1)—

- (A) any single action or conduct that violates section 2 or 3 with respect to multiple protected computers shall be treated as a single violation; and
- (B) any single action or conduct that violates more than one paragraph of section 2(a) shall be considered multiple violations, based on the number of such paragraphs violated.

(c) REQUIRED SCIENTER.—Civil penalties sought under this section for any action may not be granted by the Commission or any court unless the Commission or court, respectively, establishes that the action was committed with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive or violates this Act.

(d) FACTORS IN AMOUNT OF PENALTY.—In determining the amount of any penalty pursuant to subsection (a) or (b), the court shall take into account the degree of culpability, any history of prior such conduct, ability to pay, effect on ability to continue to do business, and such other matters as justice may require.

(e) EXCLUSIVENESS OF REMEDIES.—The remedies in this section (and other remedies available to the Commission in an enforcement action against unfair and deceptive acts and practices) are the exclusive remedies for violations of this Act.

(f) EFFECTIVE DATE.—To the extent only that this section applies to violations of section 2(a), this section shall take effect upon the expiration of the 6-month period that begins on the date of the enactment of this Act.

**SEC. 5. LIMITATIONS.**

## (a) LAW ENFORCEMENT AUTHORITY.—Sections 2 and 3 shall not apply to—

(1) any act taken by a law enforcement agent in the performance of official duties; or

(2) the transmission or execution of an information collection program in compliance with a law enforcement, investigatory, national security, or regulatory agency or department of the United States or any State in response to a request or demand made under authority granted to that agency or department, including a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a court order, or other lawful process.

## (b) EXCEPTION RELATING TO SECURITY.—Nothing in this Act shall apply to—

(1) any monitoring of, or interaction with, a protected computer—

(A) in connection with the provision of a network access service or other service or product with respect to which the user of the protected computer is an actual or prospective customer, subscriber, registered user, or account holder;

(B) by the provider of that service or product or with such provider's authorization; and

(C) that involves or enables the collection of information about the user's activities only with respect to the user's relationship with or use of such service or product,

to the extent that such monitoring or interaction is for the purpose of network security, computer security, diagnostics, technical support or repair, network management, authorized updates of software, or for the detection or prevention of fraudulent activities; or

(2) a discrete interaction with a protected computer by a provider of computer software solely to determine whether the user of the computer is authorized to use such software, that occurs upon—

(A) initialization of the software; or

(B) an affirmative request by the owner or authorized user for an update of, addition to, or technical service for, the software.

## (c) GOOD SAMARITAN PROTECTION.—

(1) IN GENERAL.—No provider of computer software or of interactive computer service may be held liable under this Act on account of any action voluntarily taken, or service provided, in good faith to remove or disable a program used to violate section 2 or 3 that is installed on a computer of a customer of such provider, if such provider notifies the customer and obtains the consent of the customer before undertaking such action or providing such service.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed to limit the liability of a provider of computer software or of an interactive computer service for any anti-competitive act otherwise prohibited by law.

(d) LIMITATION ON LIABILITY.—A manufacturer or retailer of computer equipment shall not be liable under this Act to the extent that the manufacturer or retailer is providing third party branded computer software that is installed on the equipment the manufacturer or retailer is manufacturing or selling.

(e) SERVICES PROVIDED BY CABLE OPERATORS AND SATELLITE CARRIERS.—It shall not be a violation of section 3 for a satellite carrier (as such term is defined in section 338(k) of the Communications Act of 1934 (47 U.S.C. 338(k)) or cable operator (as such term is defined in section 631(a)(2) of such Act (47 U.S.C. 551(a)(2))) to—

- (1) utilize a navigation device (as such term is defined in the rules of the Federal Communications Commission);
  - (2) interact with such a navigation device; or
  - (3) transmit software to or execute software installed on such a navigation device to provide service or collect or disclose subscriber information,
- if the provision of such service, the utilization of or the interaction with such device, or the collection of or disclosure of such information, is subject to section 338(i) or section 631 of the Communications Act of 1934.

#### SEC. 6. EFFECT ON OTHER LAWS.

(a) PREEMPTION OF STATE LAW.—

(1) PREEMPTION OF SPYWARE LAWS.—This Act supersedes any provision of a statute, regulation, or rule of a State or political subdivision of a State that expressly regulates—

- (A) unfair or deceptive conduct with respect to computers similar to that described in section 2(a);
- (B) the transmission or execution of a computer program similar to that described in section 3; or
- (C) the use of computer software that displays advertising content based on the Web pages accessed using a computer.

(2) ADDITIONAL PREEMPTION.—

(A) IN GENERAL.—No person other than the Attorney General of a State may bring a civil action under the law of any State if such action is premised in whole or in part upon the defendant violating any provision of this Act.

(B) PROTECTION OF CONSUMER PROTECTION LAWS.—This paragraph shall not be construed to limit the enforcement of any State consumer protection law by an Attorney General of a State.

(3) PROTECTION OF CERTAIN STATE LAWS.—This Act shall not be construed to preempt the applicability of—

- (A) State trespass, contract, or tort law; or
- (B) other State laws to the extent that those laws relate to acts of fraud.

(4) EFFECTIVE DATE.—The preemption provided for under this subsection shall take effect, with respect to specific provisions of this Act, on the effective date for such provisions.

(b) PRESERVATION OF FTC AUTHORITY.—Nothing in this Act may be construed in any way to limit or affect the Commission's authority under any other provision of law, including the authority to issue advisory opinions (under part 1 of volume 16 of the Code of Federal Regulations), policy statements, or guidance regarding this Act.

#### SEC. 7. FTC REPORT ON COOKIES.

(a) IN GENERAL.—Not later than the expiration of the 6-month period that begins on the date on which final regulations are issued under section 9, the Commission shall submit a report to the Congress regarding the use of cookies in the delivery or display of advertising to the owners and users of computers. The report shall examine the extent to which cookies are or may be used to transmit to a third party personally identifiable information of a computer owner or user, information regarding Web pages accessed by the owner or user, or information regarding advertisements previously delivered to a computer, for the purpose of—

- (1) delivering or displaying advertising to the owner or user; or
- (2) assisting the intended recipient to deliver or display advertising to the owner, user, or others.

The report shall examine and describe the methods by which cookies and the Web sites that place them on computers function separately and together, and shall compare the use of cookies with the use of information collection programs (as such term is defined in section 3) to determine the extent to which such uses are similar or different. The report may include such recommendations as the Commission con-

siders necessary and appropriate, including treatment of cookies under this Act or other laws.

(b) **EFFECTIVE DATE.**—This section shall take effect on the date of the enactment of this Act.

(c) **PAPERWORK REDUCTION REQUIREMENTS.**—The requirements of subchapter I of chapter 35 of title 44, United States Code, shall not apply to the report required under this section.

**SEC. 8. FTC REPORT ON INFORMATION COLLECTION PROGRAMS INSTALLED BEFORE EFFECTIVE DATE.**

Not later than the expiration of the 6-month period that begins on the date on which final regulations are issued under section 9, the Commission shall submit a report to the Congress on the extent to which there are installed on protected computers information collection programs that, but for installation prior to the effective date under section 11(a), would be subject to the requirements of section 3. The report shall include recommendations regarding the means of affording computer users affected by such information collection programs the protections of section 3, including recommendations regarding requiring a one-time notice and consent by the owner or authorized user of a computer to the continued collection of information by such a program so installed on the computer. The requirements of subchapter I of chapter 35 of title 44, United States Code, shall not apply to the report required under this section.

**SEC. 9. REGULATIONS.**

(a) **IN GENERAL.**—The Commission shall issue the regulations required by this Act not later than the expiration of the 9-month period beginning on the date of the enactment of this Act. In exercising its authority to issue any regulation under this Act, the Commission shall determine that the regulation is consistent with the public interest and the purposes of this Act. Any regulations issued pursuant to this Act shall be issued in accordance with section 553 of title 5, United States Code.

(b) **EFFECTIVE DATE.**—This section shall take effect on the date of the enactment of this Act.

**SEC. 10. DEFINITIONS.**

For purposes of this Act:

(1) **CABLE OPERATOR.**—The term “cable operator” has the meaning given such term in section 602 of the Communications Act of 1934 (47 U.S.C. 522).

(2) **COLLECT.**—The term “collect”, when used with respect to information and for purposes only of section 3(b)(1)(A), does not include obtaining of the information by a party who is intended by the owner or authorized user of a protected computer to receive the information or by a third party authorized by such intended recipient to receive the information, pursuant to the owner or authorized user—

(A) transferring the information to such intended recipient using the protected computer; or

(B) storing the information on the protected computer in a manner so that it is accessible by such intended recipient.

(3) **COMPUTER; PROTECTED COMPUTER.**—The terms “computer” and “protected computer” have the meanings given such terms in section 1030(e) of title 18, United States Code.

(4) **COMPUTER SOFTWARE.**—

(A) **IN GENERAL.**—Except as provided in subparagraph (B), the term “computer software” means a set of statements or instructions that can be installed and executed on a computer for the purpose of bringing about a certain result.

(B) **EXCEPTIONS.**—Such term does not include—

(i) computer software that is placed on the computer system of a user by an Internet service provider, interactive computer service, or Internet Web site solely to enable the user subsequently to use such provider or service or to access such Web site; or

(ii) a text or data file known as a cookie, to the extent that the text or data file—

(I) is used, written to, or placed on the computer of a user by an Internet service provider, interactive computer service, or Internet website, or any entity acting with the authorization of and on behalf of such Internet service provider, interactive computer service, or Internet website; and

(II) can be read or recognized solely to return information to such Internet service provider, interactive computer service, or Internet website, or any entity acting with the authorization of and on be-



half of such Internet service provider, interactive computer service, or Internet website.

(5) COMMISSION.—The term “Commission” means the Federal Trade Commission.

(6) DAMAGE.—The term “damage” has the meaning given such term in section 1030(e) of title 18, United States Code.

(7) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—The term “unfair or deceptive acts or practices” has the meaning applicable to such term for purposes of section 5 of the Federal Trade Commission Act (15 U.S.C. 45).

(8) DISABLE.—The term “disable” means, with respect to an information collection program, to permanently prevent such program from executing any of the functions described in section 3(b)(1) that such program is otherwise capable of executing (including by removing, deleting, or disabling the program), unless the owner or operator of a protected computer takes a subsequent affirmative action to enable the execution of such functions.

(9) INFORMATION COLLECTION FUNCTIONS.—The term “information collection functions” means, with respect to an information collection program, the functions of the program described in subsection (b)(1) of section 3.

(10) INFORMATION SERVICE.—The term “information service” has the meaning given such term in section 3 of the Communications Act of 1934 (47 U.S.C. 153).

(11) INTERACTIVE COMPUTER SERVICE.—The term “interactive computer service” has the meaning given such term in section 230(f) of the Communications Act of 1934 (47 U.S.C. 230(f)).

(12) INTERNET.—The term “Internet” means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire or radio.

(13) PERSONALLY IDENTIFIABLE INFORMATION.—

(A) IN GENERAL.—The term “personally identifiable information” means the following information, to the extent only that such information allows a living individual to be identified from that information:

- (i) First and last name of an individual.
- (ii) A home or other physical address of an individual, including street name, name of a city or town, and zip code.
- (iii) An electronic mail address.
- (iv) A telephone number.
- (v) A social security number, tax identification number, passport number, driver’s license number, or any other government-issued identification number.
- (vi) A credit card number.
- (vii) Any access code, password, or account number, other than an access code or password transmitted by an owner or authorized user of a protected computer to the intended recipient to register for, or log onto, a Web page or other Internet service or a network connection or service of a subscriber that is protected by an access code or password.
- (viii) Date of birth, birth certificate number, or place of birth of an individual, except in the case of a date of birth transmitted or collected for the purpose of compliance with the law.

(B) RULEMAKING.—The Commission may, by regulation, add to the types of information described in subparagraph (A) that shall be considered personally identifiable information for purposes of this Act, except that such additional types of information shall be considered personally identifiable information only to the extent that such information allows living individuals, particular computers, particular users of computers, or particular email addresses or other locations of computers to be identified from that information.

(14) SUITE OF FUNCTIONALLY RELATED SOFTWARE.—The term suite of “functionally related software” means a group of computer software programs distributed to an end user by a single provider, which programs enable features or functionalities of an integrated service offered by the provider.

(15) TELECOMMUNICATIONS CARRIER.—The term “telecommunications carrier” has the meaning given such term in section 3 of the Communications Act of 1934 (47 U.S.C. 153).

(16) TRANSMIT.—The term “transmit” means, with respect to an information collection program, transmission by any means.

(17) WEB PAGE.—The term “Web page” means a location, with respect to the World Wide Web, that has a single Uniform Resource Locator or another single

location with respect to the Internet, as the Federal Trade Commission may prescribe.

(18) WEB SITE.—The term “Web site” means a collection of Web pages that are presented and made available by means of the World Wide Web as a single Web site (or a single Web page so presented and made available), which Web pages have any of the following characteristics:

(A) A common domain name.

(B) Common ownership, management, or registration.

#### SEC. 11. APPLICABILITY AND SUNSET.

(a) EFFECTIVE DATE.—Except as specifically provided otherwise in this Act, this Act shall take effect upon the expiration of the 12-month period that begins on the date of the enactment of this Act.

(b) APPLICABILITY.—Section 3 shall not apply to an information collection program installed on a protected computer before the effective date under subsection (a) of this section.

(c) SUNSET.—This Act shall not apply after December 31, 2013.

#### PURPOSE AND SUMMARY

H.R. 964, the Securely Protect Yourself Against Cyber Trespass Act, prohibits unfair or deceptive acts or practices related to spyware or adware programs, and requires notice and consent for the execution of information collection programs.

#### BACKGROUND AND NEED FOR LEGISLATION

The release of the Mosaic browser in January 1993, which provided the first graphical interface for navigating the Internet, is credited with bringing the Internet into the mainstream of public usage. In the intervening time, Internet usage has been transformed from an academic tool into a commercial, educational, and communications portal accessed by more than 70 percent of Americans.

It comes as no surprise that the market has responded with new technologies tailored to consumer Internet usage. Many of these technologies are designed to improve the efficiency and speed of data transfer. For example, some maximize server efficiency and thereby reduce time requirements for a Web page to load on a user’s computer. Other technologies allow Web sites to use persistent identifiers to recognize a return visitor, and thereby enhance the online experience through personalization. The unique nature of the Internet has also facilitated other beneficial technologies, such as peer-to-peer file sharing software, instant messaging, and voice-over Internet, that capitalize on the distributed network structure.

At the same time, the Committee is aware that these technologies are capable of visiting great harm on consumers and commerce when misapplied by scam artists, criminals, and others with unsavory motives. The Committee is particularly concerned about the growing use of what is commonly referred to as “spyware.” Spyware presents privacy, security, and functionality concerns for consumers. The Federal Trade Commission (FTC) has described spyware as software “that aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer’s consent, or asserts control over a computer without the consumer’s knowledge.” The Committee received testimony that spyware represents a range of software programs on a broad continuum from

the most pernicious criminal activities on one end to the less threatening but still intrusive on the opposite end.

The most serious privacy and security concerns pertain to those programs that are intended to capture a user's personal information without knowledge and consent. The Committee received testimony demonstrating the software technology and tactics of some of these programs. They include keystroke logging software that captures a user's information (passwords, Social Security numbers, account numbers, etc.) and can lead to identity theft, and monitoring software that tracks a user's online activity, such as Web sites visited. This information could be used for profiling. Other monitoring software can include audio or video capturing programs that use one's own computer video camera or microphone to watch or listen to whatever is happening around the Internet-connected computer. Furthermore, security experts and law enforcement officers report growing cooperation among spammers, virus writers, and con artists in schemes to steal financial assets from consumers through a practice known as "phishing" by which bad actors fraudulently convince users to disclose passwords and other private financial data. Software can also affect the functioning of a computer by redirecting the user to Web sites that the user does not intend to visit, preventing a user from altering settings on the computer, or using the computer to send unsolicited commercial electronic mail. The Committee is concerned that such attacks could erode the trust that makes electronic commerce and online financial transactions possible.

Techniques for deceiving consumers into downloading spyware vary. Deceptive tactics include using pop-under windows that disguise the identity of the program distributor, offering misleading or deceptive end user licensing agreements, and failing to disclose the functionality of a program. Some spyware programs masquerade as anti-spyware technology. More nefarious tactics include exploitation of security patches in a computer's operating system. Additionally, consumers who leave browser security settings on "low" open their systems to automatic "drive-by" downloads in which spyware programs are automatically downloaded when visiting certain sites.

The Committee also is concerned with the growth of abusive "adware." Adware is advertising software that can monitor online behavior and Web sites visited. Adware is often bundled, many times as a consideration, with other software that a consumer voluntarily downloads. Adware usually directs targeted advertisements to the user based on his or her online activity. The Committee does not find adware per se objectionable, so long as a consumer has given informed consent to the software installation or execution.

On the other hand, the Committee has received testimony and other information indicating that some adware has been used to push directed advertisements of material unrelated to a user's online activity and that the user finds objectionable. Adware also has been used to barrage consumers with pop-up ads that disrupt Internet usage. Many consumers have lost important data because this malware crashed their computers, or were forced to junk perfectly good computers that were so burdened with unwanted adware that they were useless. Increasingly, adware is being cou-

pled with spyware or other deceptive or malicious software programs. See, for example, the FTC case *In Re Direct Revenue LLC, et al.*, File No. 052 313 (February 2007). DirectRevenue LLC, a large distributor of adware, installs its adware on consumer's computers directly and through a large network of affiliates and sub-affiliates. According to the FTC complaint detailing charges that DirectRevenue settled, the company and its affiliates frequently offered consumers free content and software, such as screen savers, games, and utilities without disclosing adequately that downloading them would result in installation of the adware. In other instances, according to the FTC's complaint, some of DirectRevenue's affiliates exploited security vulnerabilities in Web browsers to install the adware. In addition, the FTC charged that DirectRevenue deliberately made it difficult to identify, locate, and remove the adware once it was installed. For example, DirectRevenue allegedly failed to label its pop-up ads to identify their source, stored the adware files in rarely accessed locations on consumers' hard drives, failed to list the adware in the Windows Add/Remove utility or named the adware files to resemble core systems software or applications, and installed technology on consumers' computers to secretly reinstall the adware when consumers attempted to remove it or when the adware was deleted by consumers' anti-spyware programs. In addition, when DirectRevenue provided an uninstall tool at separate Web sites, it allegedly required consumers to follow a 10-step procedure involving the download of additional software and deactivation of all third-party firewalls, thus exposing consumers' computers to security risks. The Committee supports honest online advertising but intends for the FTC to use its existing authorities and the tools in this Act to take vigorous enforcement action against unfair or deceptive acts or practices. See also, "The Plot To Hijack Your Computer," *Business Week* cover story (July 17, 2006).

The increasing popularity and convenience of e-commerce and the benefits that it brings to our national economy make it critical for the Committee and the Congress to act expeditiously to preserve the integrity of the system and thus consumer confidence. The Committee's bipartisan legislation accomplishes that goal by striking a careful balance between cracking down on abuse while preserving beneficial uses of software applications. Similar legislation passed the House by overwhelming votes in the 108th and 109th Congresses.

#### HEARINGS

The Committee on Energy and Commerce held a hearing on the legislation on March 15, 2007. The Committee received testimony from the following: Mr. Jerry Cerasale, Senior Vice President, Direct Marketing Association, Inc.; Ms. Fran Maier, Executive Director, TRUSTe; Mr. Dave Morgan, Founder and Chairman, TACODA, Inc.; Mr. Ari Schwartz, Deputy Director, Center for Democracy and Technology; and Ms. Christine A. Varney, Esquire, Hogan & Hartson LLP, on behalf of Zango.

#### COMMITTEE CONSIDERATION

On Thursday, April 19, 2007, the Subcommittee on Commerce, Trade, and Consumer Protection met in open markup session and

approved H.R. 964 for full Committee consideration, amended, by voice vote. On Thursday, May 10, 2007, the full Committee met in open markup session and ordered H.R. 964 favorably reported to the House, amended, by voice vote.

#### COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the record votes on the motion to report legislation and amendments thereto. There were no record votes taken on amendments or in connection with ordering H.R. 964 reported. A motion by Mr. Dingell to order H.R. 964 favorably reported to the House was agreed to by voice vote.

#### COMMITTEE OVERSIGHT FINDINGS

Regarding clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee held a legislative hearing and made findings that are reflected in this report.

#### STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

The goal of H.R. 964 is to protect consumers by prohibiting deceptive practices related to spyware and adware programs and by requiring notice and consent for the execution of information collection programs.

#### NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

Regarding compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 964 would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

#### EARMARKS AND TAX AND TARIFF BENEFITS

Regarding compliance with clause 9 of rule XXI of the Rules of the House of Representatives, H.R. 964 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(d), 9(e), or 9(f) of rule XXI.

#### COMMITTEE COST ESTIMATE

The Committee adopts as its own the cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

#### CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the following is the cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974:

MAY 24, 2007.

Hon. JOHN D. DINGELL, *Chairman,*  
*Committee on Energy and Commerce,*  
*House of Representatives, Washington, DC.*

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 964, the Securely Protect Yourself Against Cyber Trespass Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Susan Willie.

Sincerely,

PETER R. ORSZAG.

Enclosure.

*H.R. 964—Securely Protect Yourself Against Cyber Trespass Act*

Summary: H.R. 964 would prohibit the use of computer software (known as spyware) to collect personal information and to monitor the behavior of computer users without a user's consent. The bill would direct the Federal Trade Commission (FTC) to enforce the bill's provisions relating to spyware, including assessing and collecting civil penalties for unfair or deceptive business practices. Based on information provided by the FTC, CBO estimates that implementing the bill would increase spending by \$1 million in 2008 and \$7 million over the 2008–2012 period, assuming appropriation of the necessary amounts.

Enacting H.R. 964 could increase civil penalties and thus could affect Federal revenues, but CBO estimates that such effects would not be significant in any year. Enacting H.R. 964 would not affect direct spending.

H.R. 964 contains an intergovernmental mandate as defined in the Unfunded Mandates Reform Act (UMRA), but CBO estimates that the resulting costs to states would fall significantly below the threshold established in UNRA (\$66 million in 2007, adjusted annually for inflation).

H.R. 964 would impose private-sector mandates, as defined in UMRA, on persons who use computer programs to collect certain information from another person's computer. In addition, by preempting certain State laws, the bill would impose a mandate on private entities by eliminating any private right of action under those laws. CBO estimates that the direct cost of complying with most of those mandates would be small and fall below the annual threshold for private-sector mandates established by UMRA (\$131 million in 2007, adjusted annually for inflation). However, due to a lack of information about the number of claims that would be filed by private entities under state laws in the absence of this legislation and the value of awards in such cases, CBO has no basis to determine the loss of compensation from awards or settlements, if any. Consequently, CBO cannot determine whether the aggregate direct cost of all the mandates in the bill would exceed the annual threshold.

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 964 is shown in the following table. The costs of this legislation fall within budget function 370 (commerce and housing credit).

	By fiscal year, in millions of dollars—				
	2008	2009	2010	2011	2012
CHANGES IN SPENDING SUBJECT TO APPROPRIATION					
Estimated Authorization Level .....	1	1	1	2	2
Estimated Outlays .....	1	1	1	2	2

Basis of estimate: For this estimate, CBO assumes that the bill will be enacted during fiscal year 2007, that the necessary amounts will be provided for each year, and that spending will follow historical patterns for similar programs.

Implementing H.R. 964 would increase spending by the FTC to enforce regulations prohibiting the unlawful use of spyware, subject to the availability of appropriated funds. Based on information from the agency, CBO estimates that such activities would cost about \$1 million in 2008 and about \$7 million over the 2008–2012 period.

Enacting H.R. 964 could increase federal revenues from civil penalties assessed for committing unfair or deceptive acts or practices in commerce; however, based on information provided by the FTC, CBO estimates that any new collections would be less than \$500,000 a year.

Estimated impact on state, local, and tribal governments: H.R. 964 would preempt state laws that specifically regulate the use of spyware. This preemption constitutes a mandate as defined in UMRA. Some states may incur costs in the form of lost court settlements, however, because the bill would preserve the rights of states to enforce their own consumer protection, trespass, contract, and/or laws, CBO estimates that any such costs would fall significantly below the threshold established in UMRA (\$66 million in 2007, adjusted annually for inflation).

Estimated impact on the private sector: H.R. 964 would impose private-sector mandates, as defined in UMRA, on persons who use computer programs to collect certain information from another person's computer. The bill would require a person who transmits or executes an information collection program on someone's computer to receive prior consent from the owner or authorized user of that computer. An information collection program is defined in the legislation as computer software that (1) collects personally identifiable information and sends the information to someone else or uses such information for advertising purposes, or (2) collects information regarding the user's Internet activity and uses such information for advertising purposes, except for software collecting information within particular Web sites. The bill would require the Federal Trade Commission to provide the manner and form of the notice to obtain consent. In addition, the bill would require an information collection program installed on someone's computer to be easily identifiable and removable. Based on information provided by industry sources and the FTC, CBO expects that the direct costs of complying with those mandates would fall below the annual threshold established by UMRA for private-sector mandates (\$131 million in 2007, adjusted annually for inflation).

Also, by preempting state laws that expressly regulate the same activities covered by the bill, H.R. 964 would impose a mandate on private entities by eliminating any private right of action under those laws. The direct cost of the mandate would be the net loss

of compensation from awards and settlements in cases where the private entity could recover full compensation for its injuries only through a private right of action that would be eliminated by H.R. 964. Because of uncertainty about the number of claims that would be filed in the absence of this legislation and the value of awards in such cases, CBO cannot estimate the cost of the mandate. Consequently, CBO cannot determine whether the cost of the mandate would exceed the annual threshold established by UMRA.

Previous CBO estimate: On May 7, 2007, CBO transmitted an estimate for H.R. 1525, the Internet Spyware Prevention Act of 2007, as ordered reported by the House Committee on the Judiciary on May 2, 2007. That bill would establish a new federal crime for the use of certain computer software (spyware) to collect personal information or to commit a federal criminal offense, and would authorize the appropriation of \$40 million over the 2008–2012 period to prosecute violations of the new law.

Estimate prepared by: Federal costs: Susan Willie; Impact on state, local, and tribal governments: Theresa Gullo; Impact on the private sector: Amy Petz.

Estimate approved by: Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.

#### FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

#### ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

#### CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee finds that the Constitutional authority for this legislation is provided in Article I, section 8, clause 3, which grants Congress the power to regulate commerce with foreign nations, among the several States, and with the Indian Tribes.

#### APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

#### SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

##### *Section 1. Short title*

Section 1 establishes the short title of the Act as the “Securely Protect Yourself Against Cyber Trespass Act,” or the “Spy Act.”

##### *Section 2. Prohibition of unfair or deceptive acts or practices relating to spyware*

Section 2(a) prohibits any person who is not an owner or authorized user of a protected computer to engage in deceptive acts or practices in connection with spyware. Specifically, it prohibits the



following conduct: (1) taking control of a protected computer; (2) modifying settings related to the use of a computer or to the computer's access to or use of the Internet by altering certain information; (3) collecting personally identifiable information through the use of a keystroke logging function; (4) inducing the owner or authorized user to disclose personally identifiable information using a fraudulent Web page; (5) inducing the owner or authorized user to install a component of computer software onto the computer or preventing reasonable efforts to block the installation or execution of, or to disable, a component of computer software; (6) misrepresenting that installing a separate component of computer software or providing log-in and password information is necessary for security or privacy reasons, or that installing a separate component of computer software is necessary to open, view, or play a particular type of content; (7) inducing the owner or authorized user to install or execute computer software by misrepresenting the identity or authority of the person or entity providing the computer software; (8) inducing the owner or authorized user to provide personally identifiable information to another person by misrepresenting the identity of the person seeking the information, or without the authority of the intended recipient of the information; or (9) removing, disabling, or rendering inoperative a security, anti-spyware, or anti-virus technology installed on the computer, or (10) installing or executing on the computer software with the intent of causing a person to use such components in a way that violates any other provision of section 2.

This bill addresses software practices that affect end user computers, whether those of individual consumers or of businesses, connected to the Internet or similar public networks. Routers and other computers on the Internet interact with one another and give each other instructions regularly as part of the routine operation of the Internet. The Committee does not intend that these and other activities that occur in the network itself, rather than on the edge of the network, be covered by the bill's definitions of "computer" or "protected computer," within the meaning of section 10(3), or that they be considered "taking control" of a computer within the meaning of section 2(a)(1).

Section 2(a)(4) provides the FTC with enforcement authority against "evil-twin attacks" and Web-based phishing. It is not intended to apply in instances of legitimate trademark dispute.

Many software installations of updated security, anti-spyware, or anti-virus technologies requested by a computer user will disable or render inoperable a prior version of that software upon installation of the updated version. Section 2(a)(9) is not intended to apply to these circumstances.

Section 2(b) directs the FTC to use its authority to issue advisory opinions, policy statements, and guidance to advise companies on the parameters of this section. For example, the FTC should issue guidance on required disclosures or material omissions that would trigger liability under section 2. Section 2(b) also provides that this subsection will take effect upon the date of enactment of the Act.

Section 2(c) provides that, except as provided in subsection (b), section 2 shall take effect upon the expiration of the 6-month period that begins on the date of enactment of the Act.

*Section 3. Prohibition of collection of certain information without notice and consent*

Section 3(a) prohibits the transmission of an information collection program to a protected computer unless the program provides for notice and consent, as set forth in section 3(c), before the first execution of the information collection program and contains the functions set forth in section 3(d). It also prohibits the execution of any information collection program on a protected computer without meeting the requirements in subsections (c) and (d).

This section contemplates a single notice at the first execution of the software. If the same information collection program executes more than one time on the same protected computer, notice is required only at the initial execution. Subsequent notice is only required if the information collection program will collect or send information that is materially different from, and outside the scope of, the type or purpose set forth in the initial or, in the case of prior subsequent notice, previous notice.

Section 3(b)(1) provides a definition for “information collection program.” An information collection program is computer software that (a) collects personally identifiable information and either (1) sends such information to a person other than the owner or authorized user of the computer or (2) uses such information to deliver advertising to or display advertising on the computer; or (b) collects information regarding Web pages accessed using the computer and uses the information to deliver advertising to or display advertising on the computer. The reference to “a person other than the owner or authorized user of the computer” in section 3(b)(1)(A)(ii)(I) is intended to include the entity that transmitted or executed the information collection program.

Section 3(b)(2) provides an exception to the definition of information collection program for software collecting information regarding Internet activity within a particular Web site. Computer software that otherwise would be considered an information collection program under section 3(b)(1)(B) shall not be considered such a program if: (1) the only information collected regarding the user’s Internet activity, and used to deliver advertising to or display advertising on the protected computer, is either (A) information regarding Web pages within a particular Web site, or (B) in the case of any Internet-based search function, user-supplied search terms necessary to complete the search and return results to the user; (2) such information is not sent to anyone other than the provider of the Web site accessed or Internet-based search function, or a party authorized to facilitate the display or functionality of Web pages within the Web site accessed; and (3) the only advertising delivered to or displayed on the computer using such information is advertising on the Web pages within the Web site. This section exempts this narrow activity. It does not create a blanket exemption for Internet search functions from the notice and consent requirements of section 3. It does not exempt the collection of other Internet activity by toolbars if it is used to deliver or display ads, nor does it exempt toolbars that are downloaded onto consumers’ computers surreptitiously as figured in the FTC’s cases in the matter of Enternet Media and ERG Ventures.

This section also is intended to exempt from the requirements of section 3 HTML, Java, Java Script, Web beacons, and other similar

tools used in the everyday functioning of the Internet to the extent that they facilitate the ordinary construction of Web pages and do not collect personally identifiable information. The Committee does not intend to interfere with the benign functioning of the Internet. This exception also allows Web site providers, or their agents, to monitor activity on their Web site, and to direct advertising on their Web site based on that monitoring, without being subject to the requirements of section 3. The Committee understands that Web site owners often use internal navigation tracking for rights management, security, site management, and similar purposes not associated with malicious spyware and adware, in order to facilitate positive interactions with consumers.

Section 3(c) sets out the requirements for notice and consent with respect to information collection programs. The notice must be clear and conspicuous in plain language and clearly distinguished from any other information contemporaneously displayed. The Committee expects the notice to be simple and clear so that consumers can easily understand that software collects information about them. Section 3(c)(1)(A) is not intended to impose specific design mandates on hardware manufacturers or software developers. The intent of the provision is to require a clearly distinct notice to the extent practicable in light of the technical and functional limitations of the information collection program or the device on which it is installed and executed. The notice must also contain a statement identifying whether the information collection program collects personally identifiable information or Web pages accessed, or both. The provider of the information collection program may use the provided language or a substantially similar statement. The language “substantially similar statement” has been added to section 3(c)(1)(B) to ensure that vendors of information collection programs have adequate flexibility to tailor section 3 notices to the user experience and in light of evolving technologies and consumer expectations. The notice must provide for the user to grant or deny consent, or to simply abandon or cancel the transaction without granting or denying consent. The notice must also provide for the user to access, before granting or denying consent, a clear description of the types of information being collected, the purpose for which the information is being collected and sent, and in the case of bundled software, the identity of the programs that qualify as information collection programs under the Act. The software provider may provide access to the information required under section 3(c)(1)(D) by a link or some other Web-based mechanism. A single notice is sufficient for bundled software programs so long as it meets the requirements under section 3(c)(1)(D)(iii). Section 3(c)(1)(E) requires concurrent display of the specified information in sections 3(c)(1)(B), (C), and (D) to the extent reasonably practicable. Section 3(c)(4) grants the FTC authority to issue regulations to carry out the subsection.

Section 3(d) provides that an information collection program must contain a disable function and, if applicable, an identity function. The disable function must allow a user of the program to remove or disable operation of the program by a mechanism that is easily identifiable to the user and can be performed without undue effort or knowledge by the user of the protected computer. The Committee has included this provision because of evidence that

purveyors of spyware have infected consumers' computers with software that cannot be removed or disabled absent destruction of the computer hard drive. The Committee expects that the FTC will take ongoing action to educate consumers on the dangers of uninstallable software that may already be residing on consumers' computers without their knowledge. Section 3(d)(1) does not require information collection programs to provide users with both a remove and a disable function. Developers of information collection programs will satisfy the requirements of section 3(d)(1) so long as the program includes at least one of these options. The identity function must provide that display of an advertisement generated by information collected through the program must be accompanied by the name of the information collection program, a logogram or trademark used for the exclusive purpose of identifying the program, or a statement or other information sufficient to clearly identify the program. Section 3(d)(2)(B) directs the FTC to promulgate rules exempting from this required function the embedded display of any advertisement on a Web page that contemporaneously displays other information. Section 3(d)(3) gives the FTC authority to carry out the subsection.

Section 3(e) provides that a telecommunications carrier, provider of information or interactive computer service, cable operator, or a provider of transmission capability shall not be liable under section 3 to the extent that it transmits, routes, hosts, stores, or provides connections for an information collection program or provides an information location tool through which the owner or authorized user of a protected computer locates an information collection program.

For purposes of commercial computing networks, the "authorized user" of computer software will be the corporate licensee of the software. As a practical matter, for purposes of sections 2 and 3, the Committee understands in many instances that system administrators are the "authorized users" in the context of commercial computing networks.

Section 3(f) directs the FTC to conduct a study to determine the applicability of the information collection prohibitions of section 3 to personally identifiable information that is input directly by users in a field provided on a Web site. The FTC is directed to examine: (1) the nature of the fields for user input; (2) how the user's information is used once input and whether it is sent to a person other than the provider of the Web site; (3) whether such information is used to deliver advertisements to the user's computer; and (4) the extent of any notice provided to the user prior to such input. The FTC is required to transmit a report, including its findings and recommendations, to the House and Senate Commerce Committees not later than six months after final regulations are issued under section 9. The FTC is authorized to adopt rules granting an exemption from the requirements of this section or modifying the notice requirements of this section with respect to such information input directly by the user, if the agency finds that users have adequate notice regarding the uses of this information, and that the exemption or modification is consistent with the public interest, the protection of consumers, and the purposes of this Act. The Committee does not intend to deny consumers the important protections provided by this Act, but is willing to have the FTC take a serious look

at this issue. While the Committee understands that responsible online marketers and retailers have readily available privacy policies, the Committee has received information about abuses and enforcement actions that militate against providing an exemption without such a study and assurances that such an exemption or modification is appropriate and not contrary to the public interest, the protection of consumers, and the purposes of this Act.

#### *Section 4. Enforcement*

Section 4(a) provides that the Act shall be enforced by the FTC under the Federal Trade Commission Act and that a violation of the Act shall be treated as an unfair or deceptive act or practice violating a rule promulgated under section 18 of the Federal Trade Commission Act. Section 4 gives the FTC the discretion to seek civil penalties for violations of the Act in one of two ways: (1) seeking civil penalties of up to \$11,000 per violation under section 5(m)(1)(A) of the FTC Act; or (2) seeking civil penalties under section 4(b) of this Act. Section 4(b) establishes an alternative enforcement mechanism for pattern or practice violations of the Act. It provides for significantly higher penalties for those whom the FTC has determined engaged in a pattern or practice of violating the Act, but also directs the FTC to treat as a single violation a single action that violates the Act but affects multiple computers. It also directs that any single action or conduct that violates more than one section of 2(a) shall be considered multiple violations. The higher damages for a pattern or practice of violation may be up to \$3,000,000 for each violation of section 2 and \$1,000,000 for each violation of section 3.

Furthermore, section 4(c) provides that civil penalties sought under the Act may not be granted by the FTC or any court unless the FTC or the court, respectively, establishes that the conduct was committed with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such conduct is unfair or deceptive and is prohibited by this Act. This is the existing scienter requirement under the FTC Act. Section 4(d) directs the FTC and the court, in determining the amount of any such civil penalty, to take into account the degree of culpability, any prior history of such conduct, ability to pay, effect on ability to continue to do business, and such other matters as justice may require. The Committee expects the FTC to enforce the law to protect consumers from unfair or deceptive acts or practices involving spyware vigorously. The Committee also expects the agency to act reasonably to avoid seeking damages out of proportion to the harm caused by the offending conduct.

Section 4(e) provides that remedies available under this section and remedies available under the FTC Act are the exclusive remedies for violation of the Act.

Section 4(f) provides that the section shall take effect upon the expiration of the 6-month period that begins on the date of enactment of the Act to the extent that the section applies to violations of section 2(a).

#### *Section 5. Limitations*

Section 5(a) provides that sections 2 and 3 of the Act shall not apply to (1) any act taken by a law enforcement agent in the per-

formance of official duties, or (2) the transmission or execution of an information collection program in compliance with a law enforcement, investigatory, national security, regulatory, agency or department of the United States, or any State in response to a request or demand made under authority granted to that agency or department. The Committee intends that this section shall be interpreted to exclude from sections 2 and 3 of the Act intelligence agencies and bona fide intelligence gathering. The Committee further intends that the activities covered by this exemption shall be carried out in accordance with all other applicable laws.

Section 5(b) provides an exception for monitoring or interaction with a protected computer for legitimate security, fraud prevention, and technical support purposes. This important exemption provides that nothing in this Act shall apply to any monitoring of, or interaction with, a protected computer (1) in connection with the provision of a network access service or other service or product with respect to which the user of the protected computer is an actual or prospective customer, subscriber, registered user, or account holder, (2) by the provider of that service or product or with such provider's authorization, and (3) that involves or enables the collection of information about the user's activities only with respect to the user's relationship with or use of such service or product, to the extent that such monitoring or interaction is for the purpose of network security, computer security, diagnostics, technical support or repair, network management, authorized updates of software, or for the detection or prevention of fraudulent activities. The primary goal of this legislation is to combat fraudulent and abusive Internet practices resulting from spyware and related nefarious technologies. The Committee intends to exempt technologies that combat practices that result in fraudulent transactions. For example, companies like Experian partner with financial institutions and online retailers in providing fraud prevention software where consumers apply for credit online. It is important to ensure that these fraud detection tools are not undermined.

Section 5(b) also provides that the Act shall not apply to a discrete interaction with a protected computer by a provider of computer software solely to determine whether the user of the computer is authorized to use such software, that occurs upon initialization of the software or an affirmative request by that user for an update of, addition to, or technical service for, the software. The intent of this provision is to allow software providers to verify that requests for technical support are coming from licensed users of software.

Section 5(c), the so-called "Good Samaritan" provision, provides protection from the threat of Federal Trade Commission enforcement to the developers of anti-spyware software and services under specified circumstances. The section thus provides that no provider of an interactive computer service may be held liable "under this Act" on account of any action voluntarily taken, or service provided, in good faith to remove or disable a program used to violate section 2 or 3 that is installed on a customer's computer, if the provider notifies the customer and obtains consent before undertaking such action. This protection would not apply to litigation between private parties or to enforcement of State law by State attorneys general. The section also provides that nothing in subsection (c) shall

be construed to limit the liability of a provider of computer software or of an interactive computer service for any anti-competitive act otherwise prohibited by law.

Section 5(d) provides that a manufacturer or retailer of computer equipment shall not be liable under this Act to the extent that the manufacturer or retailer is providing third party branded computer software that is installed on the equipment that the manufacturer or retailer is manufacturing or selling. This provision does not excuse from liability a manufacturer that includes its own software on computers that it manufactures.

Section 5(e) provides a limited exemption for certain services provided by cable operators or satellite carriers. The section provides that it shall not be a violation of section 3 for a satellite carrier or cable operator to (1) utilize a navigation device, (2) interact with such a navigation device, or (3) transmit software to or execute software installed on such a navigation device to provide service or to collect or disclose subscriber information, if such actions with respect to such information are subject to section 338 or section 631 of the Communications Act of 1934. The Committee intends to avoid duplicative regulation, not to deny consumers the protections afforded by this Act. Accordingly, if there is a provision in Section 3 of this Act that does not have a corollary in Section 631 of the Communications Act, then the scope of this exemption would be limited to what the Federal Communications Commission actually has required of cable operators. The Committee expects the FTC to consult with the Federal Communications Commission in connection with interpretation and enforcement of this provision.

#### *Section 6. Effect on other laws*

Section 6(a) provides that the Act supercedes any provision of a statute, regulation, or rule of a State or political subdivision that expressly regulates deceptive conduct with respect to computers similar to that of section 2(a), the transmission or execution of a computer similar to that in section 3, and the use of computer software that displays advertising content based on the Web pages accessed using a computer. The section also prohibits any person other than the Attorney General of a State to bring a civil action under the law of any State if such action is premised in whole or in part upon the defendant violating any provision of this Act, but makes clear that this prohibition shall not be construed to limit the enforcement of any State consumer protection law by an Attorney General of a State. The section specifically preserves State trespass, contract, and tort law, and other State laws to the extent that those acts relate to acts of general consumer fraud. The Committee intends to preserve the ability of State Attorneys General to enforce these law as an important backstop to FTC enforcement. However, the Committee intends to preempt State legislation that makes illegal an information collection program or other computer software that displays advertising in a way that complies with this Act by simply calling it a trespass, tort, or other statute in an effort to avoid preemption. The Committee specifically intends to preempt the Utah Spyware Control Act, section 13-39-101, Utah Code Annotated 1953.

Section 6(b) preserves the FTC's authority under any other provision of law, including the authority to issue advisory opinions, policy statements, or guidance regarding the Act.

*Section 7. FTC report on cookies*

Section 7(a) requires that, no later than the expiration of the 6-month period that begins on the date on which final regulations are issued under section 9, the FTC submit a report to the Congress regarding the use of cookies in the delivery or display of advertising to the owners and users of computers. The report shall examine the extent to which cookies are or may be used to transmit to a third party personally identifiable information of a computer owner or user, information regarding Web pages accessed by the owner or user, or information regarding advertisements previously delivered to a computer, for the purpose of (1) delivering or displaying advertising to the owner or user, or (2) assisting the intended recipient to deliver or display advertising to the owner, user, or others. The report shall compare the use of cookies with the use of information collection programs, as such programs are defined in section 3, to determine the extent to which such uses are similar or different. Section 10(4)(B)(ii) contains an exception clarifying when cookies are not "computer software" subject to the requirements of section 3. The Committee understands that traditional cookies are innocuous and a part of the basic functioning of most Web sites. On the other hand, the Committee has received information about so-called "tracking" or "persistent" cookies that collect identifying information and increasingly act as spyware and adware. The Committee intends for the FTC to look into these and other functionally similar information collection programs to determine whether and, if so, how they use and transmit consumer information. The Committee also intends for the FTC to examine privacy safeguards that currently exist regarding the management of cookies by online entities.

Section 7(b) provides that the section shall take effect on the date of enactment of this Act.

Section 7(c) provides an exemption from the Paperwork Reduction Act for any such report in order to facilitate its completion within the statutory time frame.

*Section 8. FTC report on information collection programs installed before effective date*

Section 8 requires that, no later than the expiration of the 6-month period that begins on the date on which final regulations are issued under section 9, the FTC submit a report to the Congress on the extent to which there are installed on protected computers information collection programs that are not covered by the notice and consent requirements of section 3 because such programs were installed prior to the effective date under section 11(a) of the Act. The report shall include recommendations regarding the means of affording computer users affected by such programs the protections of section 3, including recommendations regarding requiring a one-time notice and consent by the owner or authorized user of a computer to the continued collection of information by such a program. Section 8 also provides an exemption from the Pa-



perwork Reduction Act for any such report in order to facilitate its completion within the statutory time frame.

#### *Section 9. Regulations*

Section 9(a) provides that any regulations issued under the Act shall be issued not later than the expiration of the 9-month period beginning on the date of enactment of this Act, and in accordance with section 553 of title 5, United States Code. The subsection also provides a standard to guide FTC rulemaking under the Act, requiring a determination that such regulations are consistent with the public interest and the purposes of this Act.

Section 9(b) provides that the section shall take effect on the date of enactment of the Act.

#### *Section 10. Definitions*

Section 10 provides definitions for terms in the Act including “collect,” “computer software,” “disable,” “personally identifiable information,” “transmit,” “unfair or deceptive acts or practices,” “Web page,” and “Web site.”

The definition of “collect” makes clear that personally identifiable information that is input by the user of a protected computer and transferred to the recipient, or stored on the protected computer in a manner such that it is accessible by such intended recipient, is outside the scope of section 3 of the Act. This is intended to facilitate ease of use for consumers and providers of Internet services or Web sites. The Committee intends the exclusion from “collect” to be based on active conduct on the part of the computer user. The mere acceptance of an end user license agreement by a computer user would not be sufficient to meet this test of active conduct.

The definition of “computer software” makes clear that such term does not include software placed on the computer system of a user by an Internet service provider, interactive computer service, or Internet Web site solely to enable the user subsequently to use such provider or service or to access such Web site. The term also does not include text or data files known as cookies to the extent that such text or data file: (1) is used, written to, or placed on the computer of a user by such provider, service, or Web site, or any entity acting with the authorization of and on behalf of such provider, service, or Web site, and (2) can be read or recognized solely to return information to such provider, service, or Web site, or any entity action with the authorization of and on behalf of such provider, service, or Web site. The Committee intends to offer an amendment during Floor consideration to clarify that computer software does not include a cookie or any other type of text or data file that solely may be read or transferred by a computer.

#### *Section 11. Applicability and sunset*

Section 11 provides that, except as otherwise provided in the Act, the Act shall take effect 12 months after the date of enactment, and further that it will sunset on December 31, 2013. Section 10 also provides that the notice and consent requirements of section 3 shall not apply to an information collection program installed on a protected computer before the effective date of the Act.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED  
H.R. 964 does not amend any existing Federal statute.

